UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,209	02/03/2006	Wilhelmus Franciscus Johanne Verhaegh	NL031006	9671

22885 7590 01/07/2009

MCKEE, VOORHEES & SEASE, P.L.C.
801 GRAND AVENUE
SUITE 3200
DES MOINES, IA 50309-2721

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
01/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/567,209	VERHAEGH ET AL.	
	Examiner	Art Unit	
	Christopher C. Johns	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. Claims 1-13 are pending.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1-5, 11, and 13 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

4. In the broadest reasonable interpretation of the claims, independent claims 1, 11, and 13 could potentially be nothing more than computer software and arrangements of data. Claim 1 recites a "server" and "computation means", both of which are merely computer software. Claim 11 recites "a server", which can be merely computer software. Claim 13 merely recites "an indication", which is just data (as the "medium" cannot be said to "*comprise*...performing"). Computer software is not a statutory class of subject matter. See MPEP §2106.01.

5. Claims 6-10 and 12 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

6. Based on Supreme Court precedent[1] and recent Federal Circuit decisions[2], a §101 process must (1) be tied to a machine (e.g. a particular apparatus) or (2) transform underlying

---

[1] *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876).
[2] See especially *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008) (*en banc*).

subject matter (such as an article or materials) to a different state or thing.[3] If neither of these requirements is met by the claim(s), the method is not a patent eligible process under 35 U.S.C. §101.

7. In this particular case, independent claims 6 and 12 do not recite a tie to a particular machine, nor do they transform underlying statutory subject matter.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1 and 4-13 are rejected under 35 U.S.C. 102(b) as being anticipated by "Collaborative Filtering with Privacy", a paper by John Canny, in the Proceedings of the 2002 IEEE Symposium on Security and Privacy (hereafter "Canny").

10. As per claims 1, 6, 11, 12, and 13, Canny discloses:

11. encrypted first data from a first user, and encrypted second data from a second user (section 3.2 – "each user has data values…each value is a standard El-Gamal encryption..."); 12. server configured to obtain the encrypted first and second data (Abstract: "our system can be implemented with untrusted servers"), the server being precluded from decrypting the encrypted first and second data, and from revealing identities of the first and second users to

[3] The Supreme Court recognized that this test is not necessarily fixed or permanent and may evolve with technological advances. *Gottschalk v. Benson*, 409 U.S. 63, 71 (1972).

each other (Abstract: "we describe an algorithm whereby a community of user can compute a public 'aggregate' of their data that does not expose individual users' data");

13. computation means to obtain a similarity value between the first and second data, said computation comprising directly calculating either an encrypted inner product between the first and second data or an encrypted sum of shares of the first and second data (page 5, section 3 - "Vector Summation of Encrypted Data");

14. wherein the first and second data is anonymous to the second and first users respectively, the similarity value providing an indication of a similarity between the first and second data (Abstract: "the aggregate allows personalized recommendations to be computed by members of the community, or by outsiders"; section 2.1, "Given a vector of user preferences *P*, the most likely pair (*x*,*n*)…").

15. As per claim 4, Canny discloses:

16. computation means to obtain an encrypted inner product between the first data and the second data, or encrypted sums of shares of the first and second data in the similarity value (section 1.2 - "Collaborative filtering using SVD is not new"), and the server is coupled to a public-key decryption server for decrypting the encrypted inner product or the sums of shares and obtaining the similarity value (section 3.2 – "each value is a standard El-Gamal encryption of the exponentiation").

17. As per claim 5, Canny discloses:

18. the similarity value is obtained using a Pearson correlation or a Kappa statistic (section 5.3 – "For instance, a Pearson correlation and personality diagnosis use the entire user dataset to generate new recommendations")

19. As per claim 7, Canny discloses:

20. first or second data comprises a user profile of the first or second user respectively (Abstract – "e-commerce and…direct recommendation applications"), the user profile indicating user preferences of the first or second user to media content items (section 1 – "personalized purchase recommendations [about] restaurants, bars, movies, and interesting sights").

21. As per claim 8, Canny discloses:

22. first or second data comprises user ratings of respective content items (Abstract – "e-commerce and…direct recommendation applications"; section 1 – "personalized purchase recommendations [about] restaurants, bars, movies, and interesting sights").

23. As per claim 9, Canny discloses:

24. using the similarity value to obtain a recommendation of a content item for the first or second user (Abstract – "an algorithm whereby a community of users can compute a public 'aggregate' of their data that does not expose individual users' data. The aggregate allows personalized recommendations to be computed by members of the community…"; section 2.1 – "Given a vector of user preferences *P*…").

25. As per claim 10, Canny discloses:

26. recommendation is performed using a collaborative filtering technique (See title of the paper, 1st sentence of Abstract, and section 1).

Claim Rejections - 35 USC § 103

27. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

28. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Canny, in view of the Paillier cryptosystem.

29. As per claim 2, Canny teaches:

30. the second user calculates, through computational means, an encrypted inner product between the first data and the second data (section 1.2 – Canny discloses that collaborative filtering through Singular Value Decomposition (SVD) is well-known and "not new"), and provides the encrypted inner product to the first user via the server, the first user decrypting the encrypted inner produce for obtaining the similarity value through computational means (Canny does not explicitly disclose that the SVD of the data is encrypted, since it only mentions that the usage of SVD for collaborative filtering is non-novel. Canny's goal is to provide for a private system where information cannot be leaked. Paillier teaches a cryptosystem. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the data in an SVD collaborative filtering system, because of the want to provide for privacy and

security of the data. A person having ordinary skill in the art would appreciate the advantage that comes from this – namely, that the data communicated between users would be protected from those who would attempt to steal personal information from it. Decrypting the data would be necessary as is inherent with any encrypted data).

31. As per claim 3, Canny teaches:

32. computation means is realized using a Paillier cryptosystem, or a threshold Paillier cryptosystem using a public key-sharing scheme (Appendix A, page 12, where the system uses "cryptographic homomorphism" for the computation of the vector sums. It does not explicitly mention using a Paillier cryptosystem or a threshold Paillier cryptosystem for the computation. The Paillier cryptosystem, published in EUROCRYPT in 1999, is a homomorphic public-key cryptosystem that is based on composite degree residuosity classes. In the original paper, on page 236, Paillier notes that the system is useful for self-blinding data, and, on page 235, that it possesses additive homomorphic properties (meaning that data can be added to encrypted data without needing to decrypt the original data). The system in Canny does not explicitly use the Paillier cryptosystem for its computations. However, the Paillier system is a cryptosystem that would do exactly what the system in Canny desires – it is a homomorphic cryptosystem that allows for self-blinding. The motivation to use the Paillier system exists because it is perfectly suited for Canny's needs, and would be a simple substitution for Pedersen's scheme (cf. section 3.1, "After applying Pedersen's protocol…"). Therefore, it would have been obvious to one skilled in the art at the time of the invention to use the Paillier cryptosystem in the system in Canny, because of the interchangeability and the motivating statements in the Paillier

publication. A person having ordinary skill in the art would recognize the advantage that comes from using Paillier as a cryptosystem in Canny, namely that the system in Canny would preserve privacy appropriately).

Claim Interpretation

33. In accordance with MPEP §2111.01, the Examiner has interpreted the meaning of claim limitations in accordance with their "plain meaning", unless such terms have been defined explicitly in the specification.

34. Claims 1 and 11 are noted for their usage of the functional language "configured to". It is believed that Applicants intend "configured to" to mean "programmed to" since "configured to" is functional language and therefore given less patentable weight. In light of the notice function of the claims, the Examiner respectfully requests changing "configured to" to "programmed to" where a positive recitation is desired[4].

35. Claims 6, 11, and 12 are noted for their use of "enabling" and "enable". These elements confer no patentable weight, as anything that "enables" an action merely does not prevent said action from being performed. As such, any claim limitations following these words are seen as an optional limitations. Optional or conditional elements do not narrow claims because they can always be omitted. See *In re Johnston*, 435 F.3d 1381, 77 USPQ2d 1788, 1790 (Fed. Cir. 2006)

[4] See MPEP §2114 - "While features of an apparatus may be recited either structurally or functionally, claims directed to an apparatus must be distinguished from the prior art in terms of structure rather than function" (emphasis mine). The Manual then cites important precedent: "In re Schreiber, 128 F.3d 1473, 1477-78, 44 USPQ2d 1429, 1431-32 (Fed. Cir. 1997) (The absence of a disclosure in a prior art reference relating to function did not defeat the Board's finding of anticipation of claimed apparatus because the limitations at issue were found to be inherent in the prior art reference); see also In re Swinehart, 439 F.2d 210, 212-13, 169 USPQ 226, 228-29 (CCPA 1971); In re Danly, 263 F.2d 844, 847, 120 USPQ 528, 531 (CCPA 1959). "Apparatus claims cover what a device is, not what a device does." Hewlett-Packard Co. v. Bausch & Lomb Inc., 909 F.2d 1464, 1469, 15 USPQ2d 1525, 1528 (Fed. Cir. 1990)."

("As a matter of linguistic precision, optional elements do not narrow the claim because they can always be omitted"), and MPEP §2106 II C, which states "Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation" (emphasis in original text).

Response to Arguments

36. Applicants' arguments with respect to claims 1-13 have been considered but are moot in view of the new ground of rejection. They appear to argue limitations that were not previously in the claims – as they have been fully addressed in this Office Action, the arguments are overcome.

37. As for Applicants' arguments concerning Canny, the Examiner disagrees. Were the system in Canny to currently have one user ($n = 1$), and a second user were added to the data set (as in section 3), the first user's data could be compared to the second user's data (as the second user's data is not yet part of the set).

Conclusion

38. **Examiner's Note:** Although Examiner has cited particular columns, line numbers and figures in the references as applied to the claims above for the convenience of the applicant(s), the specified citations are merely representative of the teaching of the prior art that are applied to specific limitations within the individual claim and other passages and figures may apply as well. It is respectfully requested that the applicant(s), in preparing the response, fully consider the items of evidence in their entirety as potentially teaching all or part of the claimed invention, as

well as the context of the passage as taught by the prior art or disclosed by the Examiner. Furthermore, it must be noted that the documents cited on any enclosed PTO-892 or PTO-1449 form are cited in their entirety.

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is (571)270-3462. The examiner can normally be reached on Monday - Friday, 9 am to 5 pm.

40. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

41. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher C Johns
Examiner
Art Unit 3621

CCJ

/EVENS J. AUGUSTIN/
Primary Examiner, Art Unit 3621